ActZero

Cybersecurity Vendor Evaluation Package

Questions, Criteria, Rubric & Resources

What is Included in this Package?

This package includes various documents to support your objective evaluation of cybersecurity capabilities. They enable a deeper understanding of the qualitative differences between cybersecurity features, than feature comparison charts, or "yes/no" questions. They include:

- A list of probing questions, and what you can glean from them
- A rubric to evaluate / score the answers
- A template to populate scores across multiple vendors, and weight the features/ capabilities most important to your organization
- A list of resources to better understand measures of cybersecurity effectiveness

Why Should I Use It?

This template enables you to assess the outcomes and methods of cybersecurity providers you are considering, such as those offering Managed Detection and Response (MDR) Services.

By asking probing questions, and evaluating the answers against the criteria (rubric) provided, you can take an objective approach to your cybersecurity procurement process, to find the provider that best suits the needs of your organization.

With machine- learning enabled services quickly eroding the relevance of ‘legacy metrics’ like MTTD (discussed in more detail in our paper Contextualizing Mean Time Metrics to Improve Evaluation of Cybersecurity Vendors) and with response capabilities happening near-instantly, that proactive/preventative (“Left of Boom”) capabilities are more important than ever before.

How to Use This Package:

- See the questions and the reasons for asking them on the next page.
- Ask security providers to answer those that apply to your organization.
- Use the answer sheet to record the answers.
- Compare the answers to the rubric to score each vendor you are evaluating.
- Rank the provider using the cumulative score; you can use this to compare providers and make a more objective decision.
- Use the resources at the end of the document to better understand other quantitative measures for your cybersecurity practice.

Probing Questions	Reasons for Asking
How many kinds of log sources can your machine learning (ML) operate on?	Many vendors claim to use machine learning; this question helps you separate the talk from the walk, and understand which of your log sources they will be able to leverage.
What proportion of your detections leverage machine learning?	Similarly, MSSPs like to claim use of machine learning, when they may be limited to only a few detections while the lion's share are just signature-based or heuristic-based.
How would you describe your data science team?	Any vendor claiming to use AI or ML will need an in-house bench of comprehensive capabilities to do so. If they outsourced, or white-labelled, they may not be able to update their models along with new threats.
Does it include those with expertise in security engineering?	Data expertise is necessary, but not sufficient. For a solution to be truly effective, you need the synergistic combination of expertise in both data science and security engineering.
How does your service enable proactive hardening of my environment?	Being able to react to threats that have landed is table stakes in MDR. But without a proactive element, to harden your systems from attack to reduce your risk profile over time, you will always be 'under siege.'
What type of Response can I expect from you?	Not all responses are created equal. Some vendors will simply send an email, while others take action on your behalf - while others still take automated action at machine-speed. Understanding the nature of the response provided, and what is required of your own team, is pivotal.

Probing Questions	Reasons for Asking
What is the False Positive Rate?	Anybody familiar with a SIEM will understand that if there are too many false positives, the cost of operating the solution, and the risk of real alerts being lost in the noise, are very high.
Are automated Responses tied to the detections or just manual review?	For responses to be automated, a vendor must be confident that they are truly indicative of compromise, rather than false positives. The answer to this question can provide insight into the quality of detections.
How often are the teams able to release new detections?	This question should help separate providers that are able to adapt to new threats from those borrowing their ML capabilities from others.
Does your Machine Learning work on All Endpoint OS's?	This question helps you understand whether the benefits of machine learning are applicable to your endpoints, especially if you're using MacOS or Linux.
How about Network Data?	Similarly, this question helps you understand the rigor behind the vendor's protection of the network vector.
What Clouds does it work on?	And, while many vendors claim cloud coverage, understanding which SaaS and IaaS specifically are covered can help determine whether this claim applies to you.

Resources:

Remember, if you do opt to use mean times (or other vendor-provided measures) in your evaluation of cybersecurity vendors, or your own cybersecurity practice, take them in context (along with their shortcomings). We have resources that help you to understand them:

- Check out our Cybersecurity KPI Matrix to see the formulas, units, definitions, and use cases for cybersecurity KPIs.
- Check out our Cybersecurity KPIs for Your Maturity Level white paper for definitive guidance on evaluating and improving your cybersecurity practice via comprehensive reporting and visibility.
- Or, to hear why Mean Times aren't applicable to every situation/environment/vendor, check out Contextualizing Mean Time Metrics to Improve Evaluation of Cybersecurity Vendors.

ActZero challenges cybersecurity coverage for SMB and mid-market companies. Our Intelligent MDR provides 24/7 monitoring, protection and response support that goes well beyond other third-party software solutions. Our teams of data scientists leverage cutting-edge technologies like AI and ML to scale resources, identify vulnerabilities and eliminate more threats in less time. We actively partner with our customers to drive security engineering, increase internal efficiencies and effectiveness and, ultimately, build a mature cybersecurity posture. Whether shoring up an existing security strategy or serving as the primary line of defense, ActZero enables business growth by empowering customers to cover more ground.

TALK TO AN EXPERT

TORONTO
5045 South Service Rd, Suite 300
Burlington, Ontario, L7L 5Y7

MENLO PARK
2882 Sand Hill Rd, Suite 115
Menlo Park, California 94025

SEATTLE
Hawk Tower
255 S King St, Suite 800
Seattle, Washington 98104

actzero.ai | info@actzero.ai | 1 (855) 917-4981